ABSTRACT:

An input data block is cryptographically converted into an output data block; by performing a non-linear operation on the input data block using an S-box based on permutations. The S-box is associated with a set of at least two permutations. Each time before the S-box is used, one of the permutations is (pseudo-)randomly selected from the set of permutations and used for the conversion.

Fig. 3